Dr.WEB®
Light
für Android

Defend what you create

Benutzerhandbuch

© Doctor Web, 2015. Alle Rechte vorbehalten

Das im vorliegenden Dokument enthaltene Material ist Eigentum von Doctor Web und dient ausschließlich der persönlichen Nutzung durch Produktkäufer. Kein Teil des vorliegenden Dokumentes darf ohne Quellenangabe reproduziert, auf einer Netzwerkressource untergebracht oder mittels Kommunikationskanälen und Massenmedien verbreitet werden, ausgenommen der Nutzung für persönliche Zwecke.

WARENZEICHEN
Dr.Web, SpIDer Mail, SpIDer Guard, CureIt!, CureNet!, AV-Desk und Dr.WEB Logos sind eingetragene Warenzeichen von Doctor Web in Russland und/oder anderen Ländern. Alle sonstigen eingetragenen Warenzeichen, oder Logos und Firmennamen, die im vorliegenden Dokument erwähnt sind, sind Eigentum ihrer jeweiligen Inhaber.

HAFTUNGSAUSSCHLUSS
Unter keinen Umständen haften Doctor Web und seine Lieferanten für die im vorliegenden Dokument enthaltenen Fehler und/oder Auslassungen sowie für Schäden des Produktkäufers (direkte oder indirekte Schäden einschließlich Gewinnausfällen), die sich dadurch ergeben.

Dr.Web Light für Android
Version 9.00.5
Benutzerhandbuch
05.08.2015

Doctor Web, Hauptsitz Russland
Tretja ul. Jamskogo polja 2, Gebäude 12A
125124 Moskau
Russische Föderation

Webseite: www.drweb.com
Telefon: +7 (495) 789-45-87

Nähere Informationen zu den regionalen Vertretungen und Büros finden Sie auf unserer Webseite.

Doctor Web

Doctor Web ist ein russischer Anbieter hauseigener IT-Sicherheitslösungen.

Doctor Web bietet effektive Antivirus- und Antispam-Lösungen sowohl für staatliche Einrichtungen und große Unternehmen als auch für private Benutzer.

Die Antivirensoftware von Dr.Web wird seit 1992 entwickelt. Die Antivirus-Lösungen zeigen immer wieder hervorragende Leistungen bei der Entdeckung von Malware und entsprechen den weltweiten Sicherheitsnormen.

Zertifikate und Auszeichnungen sowie ein global weit verbreitetes Nutzer-Netzwerk zeugen vom besonderen Vertrauen der Kunden in unsere Produkte.

Wir danken allen Benutzern für ihre Unterstützung und Treue in Dr.Web Produkte!

Inhaltsverzeichnis

Kapitel 1. Einführung 5

- Symbole und Hervorhebungen 5
- Hauptfunktionen der App 5
- Systemanforderungen 6

Kapitel 2. Installation und Deinstallation 7

- App installieren 7
- App deinstallieren und aktualisieren 8

Kapitel 3. Mit der Arbeit beginnen 10

- App starten und beenden 10
- Oberfläche 10
- Widgets 11
- Benachrichtigungen 12

Kapitel 4. Programmfunktionen und -einstellungen 14

- Permanenter Virenschutz 14
- Überprüfung auf Anforderung des Benutzers 15
- Neutralisierung der Bedrohungen 17
- Bedrohungen bei Systemanwendungen entdecken 18
- Sperr-Software bearbeiten 19
- Aktualisierung 20
- Quarantäne 21
- Statistik 22

Schlagwortregister 23

Kapitel 1. Einführung

Vielen Dank, dass Sie sich für **Dr.Web *Light* für Android** (nachfolgend **Dr.Web *Light*** genannt) entschieden haben! Diese Antivirenlösung bietet einen zuverlässigen Schutz für mobile Geräte unter Android™ vor diversen Arten von Schadsoftware, welche die Sicherheit mobiler Geräte bedrohen.

Im Programm wurden die meist fortgeschrittenen Konzepte und Technologien von **Doctor Web** eingesetzt, mit denen sich die Malware-Objekte, durch welche die Funktion und Informationssicherheit des Geräts gefährdet werden können, entdecken und desinfizieren lassen.

Dr.Web *Light* verwendet die Technologie Origins Tracing™ for Android, mit der schädliche Programme auf Android-Geräten rechtzeitig erkannt werden. Es ist die einzigartige Technologie zur Erkennung böswilliger Programme für Android-Plattformen. Diese Technologie sorgt dafür, dass neue Virenfamilien aufgrund der schon bestehenden Kenntnisse über herkömmliche Bedrohungen entdeckt werden können. Mit Origins Tracing for Android lassen sich sowohl neu kompilierte Viren wie Android.SMSSend order Android.MobileSpy, als auch die mit Android.ADRD, Android.Geinimi order Android.DreamExploid infizierten Anwendungen, erkennen. Die mit Hilfe von Origins Tracing for Android entdeckten Bedrohungen erhalten den Namen Android.VirusName.origin.

In diesem Handbuch finden Nutzer mobiler Android-Geräte detaillierte Informationen rund um die Installation und Konfiguration von **Dr.Web *Light*** sowie Hauptfunktionen der App.

Symbole und Hervorhebungen

In der Anleitung werden folgende Bezeichnungen verwendet:

Symbol/Hervorhebung	Erläuterung
Fette Schrift	Elemente der grafischen Benutzeroberfläche und Beispiele für Eingaben, die exakt, wie im Handbuch beschrieben, durchgeführt werden müssen.
Fette grüne Schrift	Namen von **Doctor Web** Produkten oder Komponenten.
Grüne unterstrichene Schrift	Querverweise auf eine Stelle im Handbuch oder Links auf Webseiten.
Kursiv	Kursivformatierung wird zur Darstellung von Begriffen oder von variablen Platzhaltern verwendet, für die der Benutzer spezifische Werte eingeben muss. Bei Eingaben in der Befehlszeile wird die Kursivformatierung zur Darstellung von Parameterwerten verwendet.
GROSSBUCHSTABEN	Bezeichnungen der Tastaturtasten.
	Wichtiger Hinweis bzw. wichtige Warnung vor potentiell gefährlichen Situationen oder möglichen Fehlern.

Hauptfunktionen der App

Dr.Web *Light* ist eine zuverlässige Antivirenlösung für mobile Geräten unter Android. Die Anwendung realisiert folgende Funktionen:

- Permanenter Echtzeitschutz des Dateisystems (Prüfung der zu speichernden Dateien, zu installierenden Programme u a.m.)
- Alle Dateien des Systems bzw. einzelne Dateien und Ordner auf Anforderung des Benutzers scannen
- Archive scannen
- Auf Speicherkarte scannen
- Windows-Autostart-Dateien entdecken
- Bedrohungen in .lnk-Dateien (durch **Dr.Web** als **Exploit.CplInk** definiert) entdecken

- Entdeckte Bedrohungen löschen bzw. in die Quarantäne verschieben
- Das Gerät bei seiner Blockierung durch Erpesser-Software freigeben
- **Dr.Web Virendatenbanken** über das Internet aktualisieren
- Erfassung der Statistiken über erkannte Bedrohungen und Aktionen der App sowie Protokollierung der EreignisseDurch eine bequeme graphische Oberfläche lassen sich die Anwendungsparameter mit Rücksicht auf Bedürfnisse des Benutzers vollständig konfigurieren und ein optimales Schutzniveau für mobiles Endgeräte einstellen.

Dr.Web *Light* kann auch im Multi-Window Modus genutzt werden. In diesem Modus lassen sich mehrere Anwendungen in einzelnen Fenstern starten. Der Multi-Window Modus wird nur von Samsung Galaxy S III und höher sowie Samsung Galaxy Note 2 und höher unterstützt.

Systemanforderungen

Dr.Web *Light* setzt Android 4.0/4.1/4.2/4.3/4.4/5.0/5.1 voraus.

Außerdem benötigen Sie eine Internetverbindung, um Updates für Virendatenbanken herunterzuladen.

Bitte beachten Sie, dass kein korrekter Betrieb von **Dr.Web *Light*** bei Geräten mit der durch Benutzer veränderten Firmware bzw. mit Root-Zugriff (sogenannte gerootete Geräte) garantiert werden kann.

Standardmäßig wird die Anwendung im internen Speicher des Geräts installiert. Damit **Dr.Web *Light*** ordnungsgemäß funktionieren kann, sollten Sie die installierte App nicht auf einen externen Speicher verschieben.

Kapitel 2. Installation und Deinstallation

Dr.Web *Light* kann direkt über den Google Play heruntergeladen und installiert werden. Alternativ können Sie die Installationsdatei auf Ihr mobiles Gerät kopieren und anschließend starten. Um die App zu installieren, können Sie auch ein Synchronisierungsprogramm verwenden.

Die App kann über den Google Play Store bzw. mit Android-Bordmitteln deinstalliert werden.

App installieren

Dr.Web *Light* kann über Google Play sowie durch Ausführen der Installationsdatei auf dem Gerät bzw. mit Hilfe eines Programms zum Synchronisieren mit dem PC installiert werden.

Anwendung über Google Play installieren

1. Öffnen Sie Google Play und finden Sie **Dr.Web *Light***. Tippen Sie auf **Installieren**.

   Wenn **Dr.Web *Light*** im Google Play Store nicht zu finden ist, erfüllt das mobile Endgerät die minimalen Systemanforderungen nicht.

2. Es öffnet sich der Bildschirm mit den Informationen zu Zugriffsrechten, welche durch die Anwendung benötigt werden. Um richtig zu funktionieren, erfordert die App Zugriff auf folgende Daten:
   - zum Registrieren der Anwendung und Aktivieren der Lizenz wird ein Internetzugriff sowie Zugriff auf die Liste der Google-Konten auf dem Gerät benötigt;
   - damit der Datei-Wächter **SpIDer Guard** und der Scanner funktionieren, wird Zugriff auf den Gerät-Speicher, die Daten der Anwendungen und die SD-Karte sowie eine Möglichkeit zum Lesen und Schreiben von Daten benötigt;
   - zur Aktualisierung von Virendatenbanken wird ein Internetzugriff sowie Zugriff auf die Netzwerkeinstellungen des Geräts benötigt.

   Tippen Sie auf **OK**.

3. Die Anwendung wird automatisch installiert.

Um die Anwendung ohne Verwendung von Google Play zu installieren, müssen Sie eine solche Installationsart erlauben. Öffnen Sie hierzu den Abschnitt **Einstellungen** -> **Sicherheit** und setzen Sie ein Häkchen bei **Unbekannte Herkunft**. Die Installationsdatei **Dr.Web *Light*** kann von der Webseite von **Doctor Web** unter http://download.drweb-av.de/android heruntergeladen werden.

Installationsdatei auf einem Gerät starten

1. Kopieren Sie die Installationsdatei auf die SD-Karte.

   Zur Suche und Ausführung der Datei auf dem Endgerät wird ein Datei-Browser benötigt.

2. Verwenden Sie den Datei-Browser, um die Installationsdatei zu finden und auszuführen.
3. Die Anwendung wird automatisch installiert.

Installation mit Hilfe des Programms zum Synchronisieren des mobilen Endgeräts mit dem PC (z.B. HTC Sync™ u. a.)

1. Synchronisieren Sie Ihr mobiles Gerät mit dem PC.
2. Starten Sie den Anwendungsinstallations-Assistenten, der zum Umfang der Synchronisationssoftware gehört.
3. Geben Sie den Pfad der Installationsdatei auf dem Rechner an und folgen Sie den Anweisungen des Installationsassistenten.
4. Die Anwendung wird auf das mobile Gerät übertragen. Somit können Sie die Informationen dazu einsehen und die Installation akzeptieren. Nach der Bestätigung wird die Anwendung automatisch installiert.
5. Beenden Sie den Installationsassistenten der Synchronisationssoftware.

Dr.Web *Light* ist installiert und bereit zur Nutzung bereit.

Standardmäßig wird die Anwendung im internen Speicher des Geräts installiert. Damit **Dr.Web *Light*** ordnungsgemäß funktionieren kann, sollten Sie die installierte App nicht auf einen externen Speicher verschieben.

App deinstallieren und aktualisieren

Die App lässt sich über den Google Play Store auf eine neuere Version aktualisieren bzw. deinstallieren. Alternativ können Sie die App mit Android-Bordmitteln ohne Verbindung zum Internet deinstallieren.

App über den Google Play Store deinstallieren und aktualisieren

1. Öffnen Sie den Google Play Store und wählen Sie den Punkt **Meine Downloads** oder **Meine Apps** (je nach verwendeter Version des Betriebssystems) aus.
2. Tippen Sie in der Liste der auf dem Gerät installierten Anwendungen auf das Symbol von **Dr.Web *Light***.

   Wenn **Dr.Web *Light*** ohne Verwendung von Google Play installiert wurde, kann die Anwendung im Bereich **Meine Downloads** fehlen. In diesem Fall können Sie das Programm mit Betriebssystemmitteln löschen.

3. Tippen Sie auf dem Bildschirm mit Informationen zur Anwendung auf **Aktualisieren**, um eine neue Version zu installieren, bzw. auf **Deinstallieren**, um die App zu deinstallieren.
4. Bestätigen Sie die Aktualisierung/Deinstallation der Anwendung:
   - Die Vorgehensweise für die Aktualisierung der App ist identisch mit der unter App installieren beschriebenen.
   - Bei der Deinstallation der App müssen Sie einen Grund für die Deinstallation angeben und dann auf **OK** tippen. Die App wird deinstalliert.

App ohne Internetverbindung deinstallieren

1. Wechseln Sie zu **Einstellungen** -> **Apps**.
2. Tippen Sie in der Liste der auf dem Gerät installierten Anwendungen auf das Symbol von **Dr.Web *Light***.
3. Tippen Sie auf dem Bildschirm mit Informationen zur Anwendung auf **Deinstallieren**. Die App wird deinstalliert.
4. Nachdem die Deinstallation beendet ist, tippen Sie auf **OK**, um zur Liste der installierten Anwendungen zurück zu wechseln.

Die Quarantäne und das gespeicherte Ereignisprotokoll werden standardmäßig nicht gelöscht. Gegebenenfalls können Sie diese manuell aus dem Ordner Android/data/com.drweb/files auf der SD-Karte löschen.

Kapitel 3. Mit der Arbeit beginnen

Dieser Abschnitt beschreibt das Verfahren zum Starten und Beenden von **Dr.Web *Light*** sowie die Benutzeroberfläche der Anwendung.

App starten und beenden

App starten

Um **Dr.Web *Light*** zu starten, öffnen Sie den Bildschirm **Alle** und tippen Sie auf **Dr.Web *Light*** .

Beim ersten Start der App öffnet sich die Lizenzvereinbarung sowie Bestimmungen zur Übermittlung von Statistiken über die App und erkannte Bedrohungen an Server von **Doctor Web** und Google, die Sie akzeptieren müssen. Die erweiterte Version von **Dr.Web** bietet die Möglichkeit, auf die Übermittlung der Statistik zu verzichten.

App beenden

Um die Anwendung zu beenden, tippen Sie auf die **Home**-Schaltfläche .

Zum wiederholten Start der Anwendung können Sie auf das Symbol von **Dr.Web *Light*** im Bereich für zuletzt gestartete Anwendungen tippen.

Beim ersten Starten öffnet sich **Dr.Web *Light*** auf dem Hauptbildschirm. Beim wiederholten Starten öffnet sich das Programm in dem Bereich, der zuletzt aktiv war, als das Programm beendet wurde.

Oberfläche

Der Hauptbildschirm von **Dr.Web *Light*** (s. Abbildung 1) enthält Informationen zum aktuellen Sicherheitsstand des Systems und lässt auf folgende Funktionen der App zugreifen:

- **Vollversion erhalten** – ermöglicht es, Informationen zu Antivirus-Software **Dr.Web für Android (komplexer Schutz)** zu erhalten sowie diese über Google Play herunterzuladen.
- **SpIDer Guard** – damit lässt sich der permanente Virenschutz aktivieren/deaktivieren.
- **Scanner** – überprüft das System auf Anforderung des Benutzers (3 Prüfungsarten stehen zur Verfügung: schnell, vollständig und benutzerdefiniert).
- **Update** – enthält Informationen zum letzten Update und ermöglicht, die App bei Bedarf zu aktualisieren.
- **Statistik** – damit lassen sich Statistiken über entdeckte Bedrohungen und Aktionen des Programms dafür einsehen.
- **Quarantäne** – damit lassen sich die in Quarantäne verschobene Bedrohungen einsehen und bearbeiten.

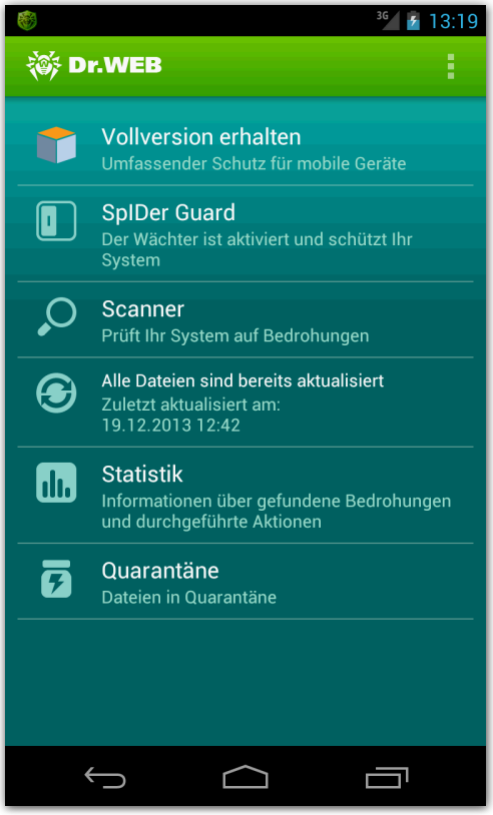


Abbildung 1. Hauptbildschirm der App

Zugriff auf das Menü und Navigation innerhalb der App

Auf den Anwendungsbildschirmen mit zusätzlichen Optionen wird das Menü mit einer Taste oben in der rechten Bildschirmecke aufgerufen. Um zum Hauptbildschirm zurückzukehren, tippen Sie auf das Logo der App in der oberen linken Ecke des Bildschirms.

Über das Menü auf dem Hauptbildschirm können Sie zu den Einstellungen der App wechseln, Hilfe aufrufen sowie Informationen über die App anzeigen.

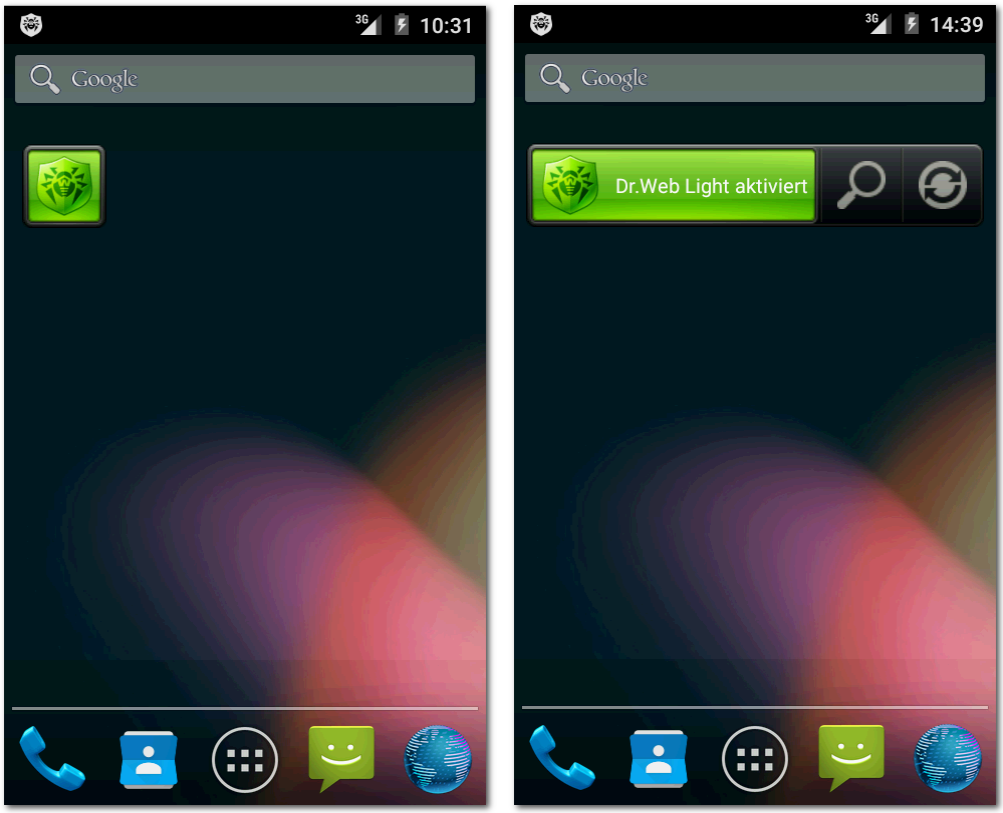
Auf dem Bildschirm mit den Informationen über die App stehen Ihnen Informationen zur App-Version zur Verfügung. In diesem Bereich finden Sie auch Links zur offiziellen Webseite von **Doctor Web** sowie zu unseren Profilen in den sozialen Netzwerken Twitter, Facebook, Instagram und Youtube.

Widgets

Damit die Nutzung von **Dr.Web *Light*** bequemer ist, können Sie spezielle Widgets auf den **Startbildschirm** Ihres Geräts bringen. Durch diese Widgets lassen sich die Hauptfunktionen der App leicht verwalten.

Widget hinzufügen

1. Die Widgets der App können mithilfe von Standard-Werkzeugen Ihres Betriebssystems hinzugefügt werden. Öffnen Sie die Liste von Widgets, die auf Ihrem Gerät hinzugefügt werden können.
2. In der Liste der verfügbaren Widgets wählen Sie eines der Widgets von **Dr.Web *Light***:
   - **Dr.Web 1x1 (klein)** – zeigt den aktuellen Schutzstatus und ermöglicht die Aktivierung/Deaktivierung von **SpIDer Guard** (s. Abbildung 2).
   - **Dr.Web 4x1 (mittelgroß)** – zeigt den aktuellen Schutzstatus, ermöglicht die Aktivierung/Deaktivierung von **SpIDer Guard**, sowie den Übergang zum Scan-Bildschirm und die Aktualisierung der Virendatenbanken (s. Abbildung 3).



Abbildungen 2 und 3. Dr.Web Widgets

Benachrichtigungen

Um schnell auf die Grundfunktionen von **Dr.Web *Light*** schnell zuzugreifen, können Sie die spezielle Benachrichtigungsleiste oben auf dem Bildschirm nutzen (s. Abbildung 4). Um diese Leiste zu aktivieren/deaktivieren, navigieren Sie zur **Benachrichtigungsleiste** im Bereich **Allgemein** (s. Abbildung 5).

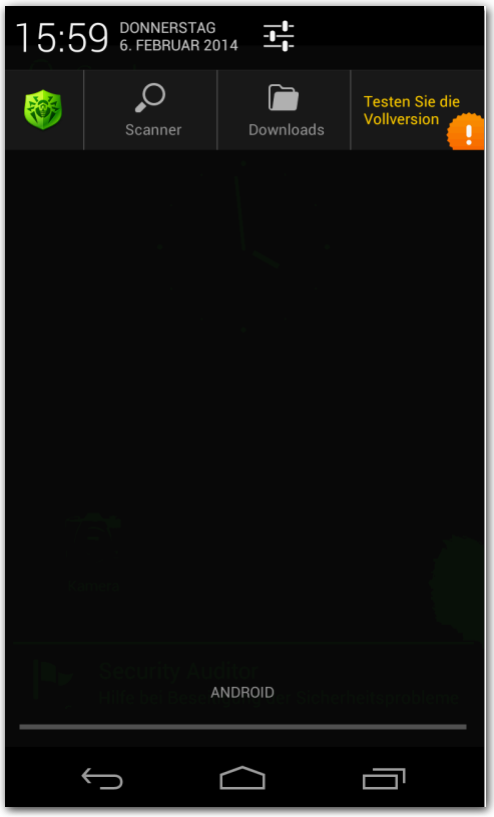


Abbildung 4. Benachrichtigungsleiste

Die Benachrichtigungsleiste bietet folgende Möglichkeiten:

- Zum Bildschirm von **Dr.Web *Light*** wechseln. Tippen Sie dazu auf das **Dr.Web**-Symbol.
- Schnelles, vollständiges bzw. benutzerdefiniertes Scannen starten. Wählen Sie dazu die Option **Scanner** und den entsprechenden Scanvorgang aus.
- Objekte scannen, die auf das Gerät geladen wurden. Wählen Sie dazu die Option **Downloads** und die Objekte zum Scannen im Ordner **Downloads** aus.
- Informationen zu **Dr.Web für Android (komplexer Schutz)** einsehen und diese Software 14 Tage kostenlos testen.

Sollten Bedrohungen erkannt werden, ändern sich die entsprechenden Symbole in der Benachrichtigungsleiste:

- – wenn die Bedrohungen durch den Scanner erkannt wurden;
- – wenn die Bedrohungen durch den Datei-Wächter **SpIDer Guard** erkannt wurden.

Unter Android 5.0 und höher wird die Benachrichtigung über eine Bedrohung in der Benachrichtigungsleiste solange über alle laufenden Anwendungen eingeblendet, bis Sie eine Aktion für die Bedrohung durchführen.

Kapitel 4. Programmfunktionen und -einstellungen

Dieser Abschnitt beschreibt die grundsätzlichen Möglichkeiten von **Dr.Web *Light***, mit denen sich die Virenprüfung konfigurieren sowie der Schutz des Geräts einrichten lässt.Um auf den Einstellungsbildschirm der App zu gelangen (s. Abbildung 5), öffnen Sie auf dem Hauptbildschrim der App das Menü und wählen Sie dann **Einstellungen**.

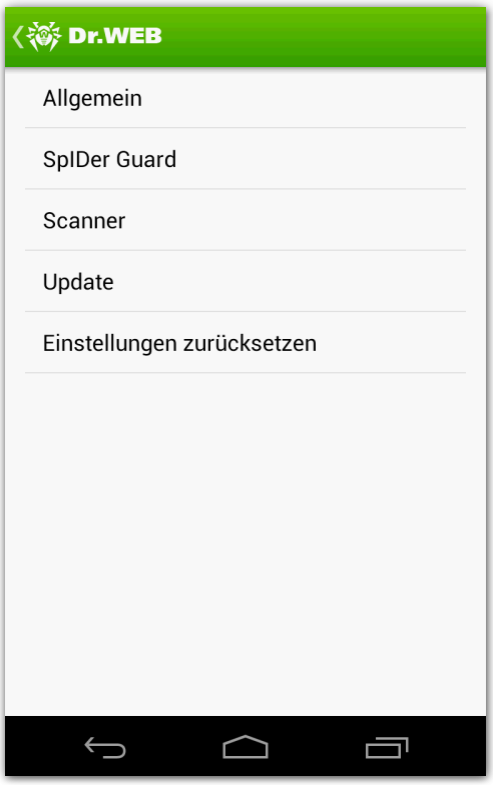


Abbildung 5. Einstellungen der App

Einstellungen zurücksetzen

Benutzerdefinierte Einstellungen können jederzeit auf Standardeinstellungen zurückgesetzt werden. Dafür müssen Sie wie folgt vorgehen:

1. Wählen Sie im Einstellungsbildschirm (s. Abbildung 5) im Bereich **Einstellungen zurücksetzen** den Punkt **Standardeinstellungen wiederherstellen** aus.
2. Bestätigen Sie die Wiederherstellung von Default-Einstellungen.

Permanenter Virenschutz

Die Hauptfunktion, die durch **Dr.Web *Light*** realisiert wird, ist eine permanente Überprüfung des Dateisystems in der Echtzeit. Dies erfolgt mithilfe von **SpIDer Guard**. Er überprüft alle Dateien, beim Versuch sie im Speicher des mobilen Geräts zu speichern. Dadurch kann das System vor Sicherheitsbedrohungen effizienter geschützt werden.

Permanenten Schutz aktivieren

Beim ersten Starten von **Dr.Web *Light*** wird der permanente Schutz automatisch nach Akzeptieren der Lizenzvereinbarung aktiviert. Um den Schutz zu deaktivieren bzw. erneut zu aktivieren, tippen Sie auf dem Hauptbildschirm der App auf **SpIDer Guard**.

Beim Aktivieren beginnt der Wächter, Ihr System zu schützen. Er funktioniert weiter unabhängig davon, ob die Anwendung gestartet ist oder nicht. Wenn eine Sicherheitsbedrohung erkannt wird, erscheint das Warnsymbol (für Android 5.0 und höher –) und eine Benachrichtigung über die erkannte Bedrohungin in der Statusleiste des Geräts. Im Benachrichtigungen-Bereich können Sie die Informationen zu Anzahl entdeckter Bedrohungen einsehen und die Liste der Bedrohungen öffnen, um Aktionen zur deren Neutralisierung auszuführen.

Der Dateiwächter wird gestoppt, wenn der Speicher Ihres Geräts im integrierten Task-Manager komplett geleert wird. In diesem Fall müssen Sie **Dr.Web *Light*** wiederholt öffnen, um ständigen Virenschutz wiederherzustellen.

Einstellungen von SpIDer Guard

Für den Zugriff auf die Einstellungen von **Dr.Web *Light*** auf dem Hauptbildschirm des Programms rufen Sie das Anwendungsmenü auf und wählen Sie den Punkt **Einstellungen**. Um den Dateiwächter zu konfigurieren, gehen Sie im Einstellungsbildschirm (s. Abbildung 5) wie folgt vor:

- Um die Prüfung von Dateien in Archiven zu aktivieren, setzen Sie ein Häkchen bei **Dateien in Archiven** im Bereich **SpIDer Guard**.

  Standardmäßig ist die Archivprüfung deaktiviert. Durch die Aktivierung der Archivprüfung kann die Operationsgeschwindigkeit des Betriebssystems beschränkt und die Batterielaufzeit reduziert werden. Dabei beeinflusst die Deaktivierung der Archivprüfung den Schutzstatus nicht, da die Installationsdateien für Android-Betriebssysteme (.apk) durch den Dateiwächter überprüft werden, unabhängig davon, welcher Wert für diesen Parameter festgelegt wurde.

- Um die Prüfung der SD-Karte bei jedem Anschließen an das Gerät zu aktivieren, setzen Sie ein Häkchen bei **SD-Karte anschließen** im Bereich **SpIDer Guard**.
- Um die Überprüfung des Systems auf Adware und PUAs (darunter auch Dialer und Scherzprogramme) zu aktivieren/deaktivieren, wählen Sie den Punkt **Optionen** im Bereich **SpIDer Guard** und setzen/wählen Sie das Häkchen bei **Adware** und **Riskware** ab.
- Um die SD-Karte auf Windows-Autostart-Dateien zu überprüfen, setzen Sie ein Häkchen bei **Autorun-Dateien** im Bereich **Allgemein**. Diese Einstellung wird auch beim Scannen auf Anforderung des Benutzers verwendet.
- Um die Anzeige des App-Symbols (für Android 5.0 und höher –) in der Statusleiste nach der Aktivierung des Wächters zu aktivieren, setzen Sie im Bereich **Allgemein** ein Häkchen bei **Dr.Web Icon**.

Statistik

Die App protokolliert Ereignisse, die mit dem Betrieb von **SpIDer Guard** (darunter Informationen über die Aktivierung/Deaktivierung, Scan-Ergebnisse und erkannten Sicherheitsbedrohungen) verbunden sind. Aktionen der App, insbesondere von **SpIDer Guard**, werden im Bereich **Aktionen** auf der Registerkarte **Statistik** nach Datum sortiert angezeigt.

Überprüfung auf Anforderung des Benutzers

Das System wird auf Anforderung des Benutzers mit Hilfe einer speziellen Komponente – eines Scanners – überprüft. Der **Dr.Web *Light*** Scanner ermöglicht das schnelle oder vollständige Scannen des Dateisystems sowie die Überprüfung einzelner Dateien und Ordner.

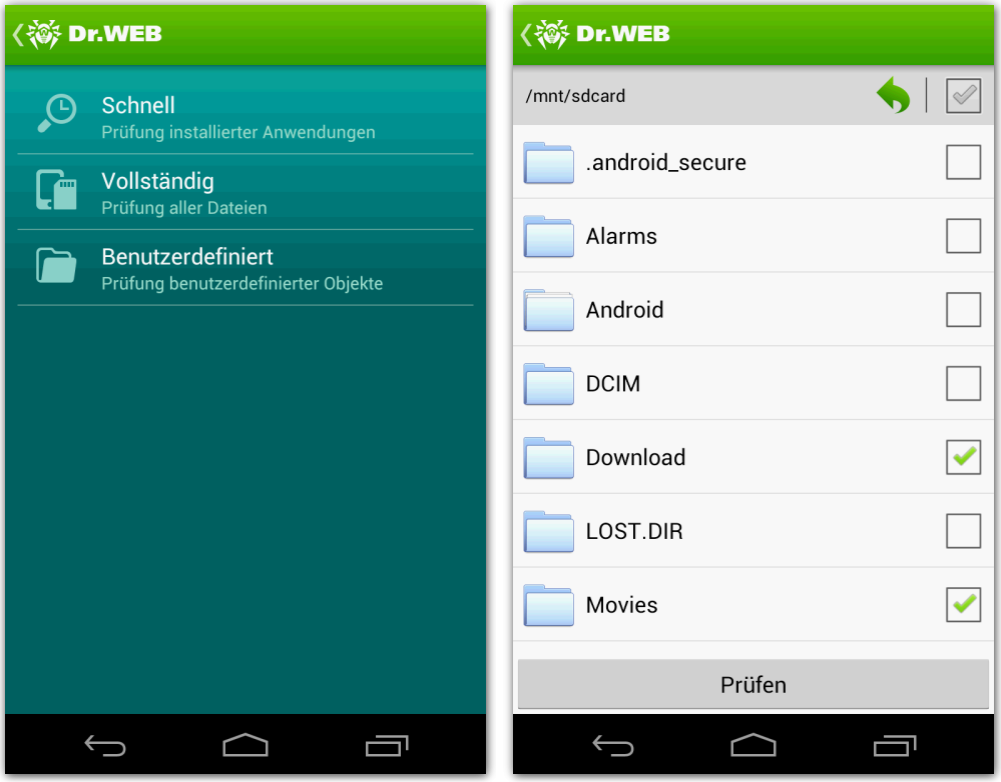
Scannen

Um das System zu scannen, tippen Sie im Hauptbildschirm auf **Scanner** und führen Sie im geöffneten

Fenster (s. Abbildung 6) eine der folgenden Aktionen durch:

- Um das Scannen installierter Anwendungen zu starten, wählen Sie den Punkt **Schnell**.
- Um das Scannen aller Dateien im System zu starten, wählen Sie den Punkt **Vollständig**.
- Um einzelne Dateien und Ordner zu überprüfen, wählen Sie den Punkt **Benutzerdefiniert**. In der geöffneten Liste mit Objekten des Dateisystems wählen Sie erforderliche Objekte aus (s. Abbildung 7) und tippen Sie auf **Prüfen**. Für die Auswahl der Objekte in der Liste können Sie die Optionen benutzen, die sich rechts über der Liste befinden und alle Elemente der Liste wählen bzw. auf die nächste höhere Ebene wechseln, um zwischen den Ordnern zu navigieren.

Nachdem das Scannen beendet wird, erscheint eine Liste entdeckter Bedrohungen auf dem Bildschirm und es wird Ihnen angeboten, Aktionen zur ihrer Neutralisierung zu wählen.



Abbildungen 6 und 7. Scanner und Fenster zur Auswahl der Scan-Objekte

Verdächtige Dateien dem Virenlabor von Doctor Web zusenden

Bei Bedarf können Sie verdächtige ZIP-Archive (eventuell Dateien mit JAR- und APK-Erweiterung), in denen Sie schädliche Programme vermuten, oder vertrauenswürdige ZIP-Archive, bei denen es sich um vermutliche Fehlalarme handelt, an das **Doctor Web** Virenlabor senden:

1. Wählen Sie die Datei in der Liste des Dateiverwaltungssystems aus (s. Abbildung 7), tippen Sie danach auf **Dem Virenlabor zusenden**.
2. Geben Sie im nächsten Fenster Ihre e-Mail-Adresse ein, wenn Sie die Ergebnisse der Analyse der zugesandten Datei erhalten möchten.
3. Wählen Sie eine der Kategorien für Ihre Anfrage aus:
   - **Verdacht auf Infizierung**, wenn Sie glauben, dass die Datei eine Bedrohung darstellt;
   - **Fehlalarm** oder **Fehlalarm der Origins Tracing**, wenn Sie glauben, dass die Datei fehlerhaft Bedrohungen zugeordnet wurde.

   Die Auswahl einer der angebotenen Kategorien im Falle des Fehlalarms erfolgt aufgrund des Namens der vermutlich in der zugesandten Datei enthaltenen Bedrohung: Enthält der Name das Suffix

".origin", so sollte die Kategorie **Fehlalarm der Origins Tracing** und in anderen Fällen - die Kategorie **Fehlalarm** gewählt werden.

4. Tippen Sie auf **Senden**.

Sie können ZIP-Archive bis zu 10 MB an das **Doctor Web** Virenlabor senden.

Scanner konfigurieren

Um den Scanner einzustellen, rufen Sie im Hauptbildschirm das App-Menü auf, wählen Sie den Menüpunkt **Einstellungen** aus und navigieren Sie anschließend zu **Scanner**. Hier stehen Ihnen die folgenden Einstellungen zur Verfügung:

- Um die Prüfung von Dateien in Archiven zu aktivieren, setzen Sie ein Häkchen bei **Dateien in Archiven im Bereich Scanner**.

Standardmäßig ist die Archivprüfung deaktiviert. Durch die Aktivierung der Archivprüfung kann die Operationsgeschwindigkeit des Betriebssystems beschränkt und die Batterielaufzeit reduziert werden. Dabei beeinflusst die Deaktivierung der Archivprüfung den Schutzstatus nicht, da die Installationsdateien für Android-Betriebssysteme (.apk) durch den Dateiwächter überprüft werden, unabhängig davon, welcher Wert für diesen Parameter festgelegt wurde.

- Um die Überprüfung des Systems auf Adware und PUAs (darunter auch Dialer und Scherzprogramme) zu aktivieren/deaktivieren, wählen Sie den Punkt **Optionen** im Bereich **Scanner** und setzen/wählen Sie das Häkchen bei **Adware** und **Riskware** ab.
- Um die SD-Karte auf Windows-Autostart-Dateien zu überprüfen, setzen Sie ein Häkchen bei **Autorun-Dateien** im Bereich **Allgemein**. Diese Einstellung wird auch bei Nutzung des Dateiwächters verwendet.

Es ist empfehlenswert, das Dateisystem regelmäßig zu scannen, z. B. wenn der Wächter einige Zeit nicht aktiv war. In der Regel reicht dabei eine schnelle Systemprüfung aus.

Statistik

Die App protokolliert Ereignisse, die mit dem Betrieb des Scanners (darunter Informationen über den Modus und Ergebnisse des Scans sowie erkannte Sicherheitsbedrohungen) verbunden sind. Aktionen der App, insbesondere des Scanners, werden im Bereich **Aktionen** auf der Registerkarte **Statistik** nach Datum sortiert angezeigt.

Neutralisierung der Bedrohungen

Liste mit Bedrohungen einsehen

Wenn der Dateiwächter **SpIDer Guard** eine Sicherheitsbedrohung erkennt, erscheint in der Statusleiste des Geräts das Warnsymbol (für Android 5.0 und höher -). Auf dem Bildschirm wird darüber hinaus eine Push-Benachrichtigung mit Informationen zu den erkannten Bedrohungen angezeigt. Tippen Sie in der Benachrichtigungsleiste auf die Benachrichtigung mit Informationen über die Anzahl entdeckter Bedrohungen, um die Liste mit allen erkannten schädlichen Objekten zu öffnen.

Unter Android 5.0 und höher wird die Benachrichtigung in der Benachrichtigungsleiste solange über alle laufenden Anwendungen eingeblendet, bis Sie eine Aktion für die Bedrohung durchführen oder die Benachrichtigung mit dem Finger wegwischen. Unter Android 5.0 und höher werden Benachrichtigungen über erkannte Bedrohungen ebenfalls auf dem Sperrbildschirm angezeigt. Vom Sperrbildschirm können Sie dann direkt die Liste erkannter Bedrohungen aufrufen.

Bei der Überprüfung Ihres Geräts durch den Scanner öffnet sich die Liste mit den entdeckten Bedrohungen automatisch, nachdem der Scanvorgang beendet wurde. Die Liste erkannter Bedrohungen kann erst dann geschlossen werden, nachdem für jede Bedrohung eine Aktion gewählt wurde.

Folgende Informationen werden für jede Bedrohung angezeigt:

- Bedrohungsname;
- Pfad der Datei, die eine Bedrohung enthält.

Für gefundene Bedrohungen, die nicht als Viren eingestuft werden, wird in Klammern der entsprechende Bedrohungstyp angezeigt: Adware, Riskware, Scherzprogramm oder Hacktool.

Aktionen für Bedrohungen verwenden

Tippen Sie in der Liste auf die Bedrohung, um alle möglichen Aktionen anzuzeigen und eine davon auszuführen. Nutzer von **Dr.Web *Light*** können eine der folgenden vier Aktionen auswählen:

- **Löschen** – die Bedrohung wird komplett aus dem Speicher des Geräts gelöscht
- **In Quarantäne** – die Bedrohung wird in einen speziellen Ordner verschoben und vom System isoliert

Wenn eine Bedrohung in der installierten Anwendung entdeckt wurde, wird es unmöglich sein, sie in die Quarantäne zu verschieben. In diesem Fall fehlt die Aktion **In Quarantäne** in der Liste.

- **Überspringen** – die Anwendung überspringt die Bedrohung und führt keine Aktion dafür aus
- **Fehlalarm melden** – Es wird Ihnen angeboten, das bedrohliche Objekt dem **Virenlabor von Doctor Web** zusammen mit der Meldung darüber, dass dieses Objekt keine Bedrohung darstellt und fälschlicherweise von dem Antivirusprogramm als verdächtig eingeschätzt wurde, zuzusenden. Um die Ergebnisse der Dateianalyse zu erhalten, geben Sie Ihre E-Mail-Adresse in dem entsprechenden Eingabefeld an und tippen Sie auf **Senden**.

Die Aktion **Fehlalarm melden** ist nur für modifizierte Bedrohungen möglich, die das Suffix „.origin" enthalten und im Systembereich gefunden wurden.

Sie können akustische Benachrichtigungen für Entdecken, Löschen und Verschieben von Bedrohungen in Quarantäne einstellen. Dafür rufen Sie auf dem Hauptbildschirm des Programms das Anwendungsmenü auf und wählen Sie den Punkt **Einstellungen.** Danach setzen Sie ein Häkchen bei **Ton** im Bereich **Allgemein** im Einstellungsbildschirm (s. Abbildung 5).

Bedrohungen bei Systemanwendungen entdecken

In manchen Fällen können die Systemanwendungen, die von Herstellern auf Ihr Gerät vorinstalliert werden, Malware-spezifische Funktionen ausführen. Somit kann **Dr.Web *Light*** diese Anwendungen beim Scannen als Sicherheitsbedrohungen beurteilen und eine entsprechende Warnung anzeigen. Die standardmäßigen Aktionen zur Neutralisierung von Bedrohungen können dabei nicht eingesetzt werden. Sie können aber wie folgt vorgehen:

- Beenden Sie die Anwendung über die Einstellungen des Geräts (tippen Sie in der Liste installierter Anwendungen auf dem Bildschirm **Einstellungen** -> **Apps** auf den Namen der Anwendung, die als

Bedrohung erkannt wurde. Tippen Sie auf dem Bildschirm mit Informationen zur App auf **Beenden erzwingen**).

Diesen Vorgang müssen Sie bei jedem Neustart Ihres Geräts wiederholen.

- Beenden Sie die Anwendung über die Einstellungen des Geräts (tippen Sie in der Liste installierter Anwendungen auf dem Bildschirm **Einstellungen** -> **Apps** auf den Namen der Anwendung, die als Bedrohung erkannt wurde. Tippen Sie auf dem Bildschirm mit Informationen zur App auf **Deaktivieren**).

Dieser Vorgang ist nur unter Android 4.0 oder höher möglich. Sie müssen diesen Vorgang nach jedem Neustart des Geräts nicht wiederholen.

- Wenn die Firmware auf Ihrem Gerät verändert wurde, können Sie es auf die Werkseinstellungen zurücksetzen und die Original-Software des Herstellers nutzen.
- Wenn Sie die Original-Software des Herstellers des mobilen Geräts nutzen, wenden Sie sich für nähere Informationen über die App an den Hersteller Ihres Geräts.
- Auf einem Gerät mit dem root-Zugriff können Sie versuchen, die Anwendung mit Hilfe spezieller Tools zu entfernen.

Des Weiteren können Sie die Benachrichtigungen über Bedrohungen, die in bekannten Systemanwendungen erkannt werden, mit Hilfe der Option **System-Anwendungen** im Bereich **Allgemeine Einstellungen** -> **Erweitert** im Einstellungsbildschirm deaktivieren (s. Abbildung 5).

Sperr-Software bearbeiten

Mit **Dr.Web *Light*** schützen Sie Ihr mobiles Gerät vor weit verbreiteten Ransomware für Android-Plattformen. Diese Art von Software ist sehr gefährlich. Damit können die auf Smartphones und Tablet-PCs als Wechseldatenträgern gespeicherten Dateien verschlüsselt werden. Der Bildschirm des mobilen Geräts kann gesperrt werden, wobei eine Nachricht mit einer Lösegeld-Forderung für Freigabe von Dateien bzw. des Geräts angezeigt wird.

Die Erpresser-Software gefährdet Fotos, Videos und Dokumente, die auf der Wechselkarte eines mobilen Geräts gespeichert werden. Darüber hinaus raubt die Ransomware unterschiedliche Informationen zu dem infizierten Gerät (darunter auch IMEI), die Daten aus dem Adressbuch (Kontaktnamen, Rufnummern und E-Mail-Adressen) und übermittelt diese an die Server der böswilligen Benutzer. Die ein- und ausgehenden Anrufe werden durch die Ransomware nachverfolgt und können dadurch gesperrt werden. Alle gesammelten Daten, darunter auch Daten über die Anrufe, werden auch an den Verwaltungsserver übermittelt.

Die erpresserische Schadsoftware wird durch **Dr.Web *Light*** erkannt und entfernt, soweit diese versucht, ins geschützte Gerät einzudringen. Die Ransomware wächst aber ständig in Anzahl und Vielfalt. Wenn die **Dr.Web Virendatenbanken** eine gewisse Zeit lang nicht aktualisiert wurden und keine Informationen zu neuen Typen enthalten, kann es vorkommen, dass die Sperrsoftware auf dem Gerät installiert wird.

Wenn das mobile Endgerät mit dem aktivierten Dateiwächter **SpIDer Guard** durch die Ransomware gesperrt wurde, können Sie wie folgt vorgehen, um das Gerät freizugeben:

1. Schließen Sie Ihr mobiles Endgerät für 5 Sekundenan eine Stromquelle an.
2. Stecken Sie innerhalb von den nächsten 10 Sekunden einen Kopfhörer ein.
3. Stecken Sie innerhalb der nächsten 5 Sekunden den Kopfhörer aus.
4. Schütteln Sie innerhalb der nächsten 10 Sekunden kräftig Ihr mobiles Endgerät.

5. **Dr.Web *Light*** beendet alle aktiven Prozesse auf dem Gerät, darunter auch den Prozess, der durch die Ransomware gestartet wurde. Danach ertönt ein kurzes Vibrationssignal (vorausgesetzt, dass diese Funktion auf dem Gerät vorhanden ist). Es öffnet sich der Bildschirm von **Dr.Web *Light***.

Bitte beachten Sie, dass die Daten anderer Anwendungen beim Beenden der aktiven Prozesse verloren gehen können, wenn diese Anwendungen bei Sperrung des Geräts aktiv waren.

6. Es wird empfohlen, die **Dr.Web Virendatenbanken** nach Freigabe des Geräts zu aktualisieren und einen schnellen Scan des Systems durchzuführen bzw. die böswillige Anwendung zu entfernen.

Aktualisierung

Zur Entdeckung von Sicherheitsbedrohungen verwendet **Dr.Web *Light*** spezielle **Virendatenbanken von Dr.Web**, die Speziallisten von **Doctor Web** mehrmals täglich mit Informationen über alle neuen Sicherheitsrisiken, denen Android-Geräte ausgesetzt sein können, aktualisieren. Die Datenbanken bedürfen einer regelmäßigen Aktualisierung, da immer neue Schadprogramme erscheinen. Dafür können die Virendatenbanken über Internet aktualisiert werden.

Auf dem Hauptbildschirm der App unter **Update** wird das Datum der letzten Aktualisierung angezeigt.

Aktualisierung

1. Um die Virendatenbanken zu aktualisieren, tippen Sie auf dem Hauptbildschirm der App auf den Abschnitt mit Informationen zu Updates.
2. Die Aktualisierung wird automatisch gestartet.

Sobald die App installiert ist, sollten Sie die Virendatenbanken aktualisieren, damit **Dr.Web *Light*** die aktuellsten Informationen zu bekannten Bedrohungen verwendet kann. Die Virensignaturen, Informationen zu deren Merkmalen und Verhaltensmustern werden sofort aktualisiert, sobald neue Bedrohungen durch Spezialisten des **Virenlabors von Doctor Web** entdeckt werden. Manchmal geschieht dies mehrmals pro Stunde.

Aktualisierungseinstellungen

Standardmäßig werden die Updates automatisch vier Mal am Tag geladen. In dem Bereich **Update** im Einstellungsbildschirm (s. Abbildung 5) können Sie die Verwendung von mobilen Netzwerken beim Herunterladen von Updates erlauben/verbieten. Damit keine mobilen Netzwerke beim Herunterladen von Updates benutzt werden, setzen Sie ein Häkchen bei **Mobiles Internet nicht benutzen**. Wenn keine aktiven Netzwerke entdeckt werden, wird es Ihnen angeboten, 3G- bzw. GPRS-Netze zu nutzen. Eventuelle Änderungen dieser Einstellung haben keine Auswirkungen auf andere Anwendungen Ihres mobilen Geräts.

Bei der Aktualisierung werden die Daten übers Netzwerk geladen. Für die Datenübertragung können zusätzliche Kosten anfallen. Mehr dazu erfahren Sie bei Ihrem Mobilfunkanbieter.

Quarantäne

Entdeckte Bedrohungen werden durch **Dr.Web *Light*** in Quarantäne – in einen speziellen Ordner, der zur deren Isolierung und sicheren Speicherung dient – verschoben.

Bedrohungen in Quarantäne behandeln

1. Zum Einsehen einer Liste der in die Quarantäne verschobenen Bedrohungen auf dem Hauptbildschirm des Programms wählen Sie den Punkt **Quarantäne**.
2. Es öffnet sich die Liste aller Bedrohungen, die sich in der Quarantäne befinden (s. Abbildung 8).
3. Tippen Sie auf eine Bedrohung in der Liste, um folgende Informationen dazu einzusehen:
   - Dateiname
   - Pfad der Datei
   - Datum der Verschiebung in die Quarantäne

   Darüber hinaus können Sie dem Link im Bereich **Informationen im Internet** folgen, um weitere Informationen zu ähnlichen Bedrohungen im Internet auf der Webseite von **Doctor Web** einzusehen.
4. Sie können eine der folgenden Aktionen für jede Bedrohung ausführen:
   - **Wiederherstellen** – um die Datei in den Ordner, in dem sich diese Datei vor ihrer Verschiebung befand, zu bringen (verwenden Sie diese Funktion nur in dem Fall, wenn kein Zweifel besteht, dass die Datei sicher ist).
   - **Löschen** – um die Datei aus der Quarantäne und aus dem System zu löschen.

Abbildung 8. Quarantäne

Größe von Quarantäne

Sie können Informationen zum Speicherplatz, der durch Quarantäne eingenommen wird, sowie zum freien Speicherplatz auf der SD-Karte einsehen. Dafür rufen Sie das Anwendungsmenü im Tab **Quarantäne** auf und wählen den Punkt **Quarantäne-Größe** aus.

Statistik

Dr.Web *Light* zeichnet Informationen über erkannte Bedrohungen und Aktionen der App auf. Um Statistiken zur App-Nutzung anzusehen, öffnen Sie auf dem Hauptbildschirm das Menü der App und wählen Sie den Punkt **Statistik** aus.

Im **Statistik**-Tab finden Sie zwei Informationsbereiche (s. Abbildung 9):

- **Insgesamt**-Bereich, der Informationen zur Gesamtzahl überprüfter Dateien, entdeckter und neutralisierter Bedrohungen beinhaltet.
- **Aktionen**-Bereich, der Informationen zu Prüfungsbeginn/-ende, Aktivierung/Deaktivierung des Wächters sowie zu entdeckten Bedrohungen und Aktionen zu deren Neutralisierung beinhaltet. Tippen Sie auf den Namen einer Bedrohung, um ihre Beschreibung auf der Webseite von **Doctor Web** abzurufen.

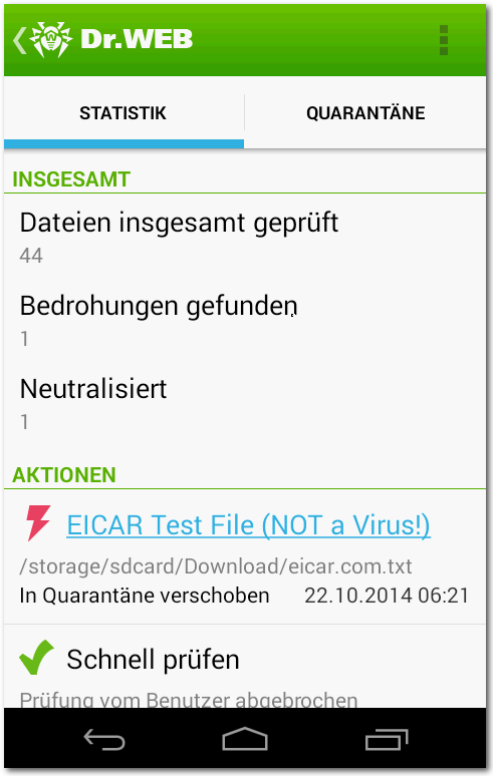


Abbildung 9. Statistik

Statistik bereinigen

Um alle erfassten Statistiken zur App zu löschen, rufen Sie das Menü der App auf und wählen Sie den Punkt **Statistik bereinigen** aus.

Ereignislog

Die App zeichnet alle Ereignisse in einem Protokoll auf, das auf der SD-Karte gespeichert und zur Analyse verwendet wird, falls die App nicht ordnungsgemäß funktioniert.

Um das Ereignislog zu speichern:

1. Tippen Sie auf das **Menü** im **Statistik**-Tab und wählen Sie den Punkt **Protokoll speichern** aus.
2. Das Log wird in der Datei DrWeb_Log.txt gespeichert. Diese Datei befindet sich im Verzeichnis Android/data/com.drweb/files auf der SD-Karte.

Schlagwortregister

A

Aktionen bei Bedrohungen 18, 19
- Akustische Benachrichtigungen 17
- Quarantäne 21

Aktualisierung
- Automatische Aktualisierung 20
- Einstellungen 20

Arbeitsbeginn 10

Autostart-Dateien 14, 15

B

Bedrohungen
- Bearbeiten 17, 18
- Sperr-Software 19
- Systemanwendungen 18

Benachrichtigungen 12

Benachrichtigungsleiste 12

Benutzerdefinierter Scan 15

D

Datei an das Virenlabor senden 15, 17, 21

Deinstallation des Programms 7, 8

Dr.Web Icon 14

Dr.Web Light 5
- Aktionen 17
- Aktualisierung 20
- Arbeitsbeginn 10
- Benachrichtigungen 12
- Deinstallation 7, 8
- Einstellungen 14
- Einstellungen zurücksetzen 14
- Ereignislog 22
- Funktionen 5, 14
- Installation 7
- Oberfläche 10
- Quarantäne 21
- Scanner 15
- SpIDer Guard 14
- Start 10
- Statistik 22
- Systemanforderungen 6
- Wächter 14
- Widgets 11

E

Einstellungen zurücksetzen 14

Ereignislog 22

F

Fehlalarm 15, 17, 21

G

Google Play 7, 8

M

Market 7, 8

O

Oberfläche 10

P

Permanenter Schutz 14

Programm installieren 7

Programm starten 10

Programmeinstellungen
- Aktualisierung 20
- Einstellungen zurücksetzen 14
- Scanner 15
- Wächter 14

Programmfunktionen 5

Q

Quarantäne
- Aktionen bei Bedrohungen 21
- Größe 21

R

Ransomware 19

S

Scan
- Benutzerdefiniert 15
- Fehlalarm 15
- Schnell 15
- Vollständig 15

Scanner
- Benutzerdefinierter Scan 15
- Einstellungen 15
- Schneller Scan 15

Schlagwortregister

Scanner
Statistik 15
Vollständiger Scan 15
Schneller Scan 15
Schutzstatus 10
Sperr-Software 19
SpIDer Guard
Aktivierung 14
Einstellungen 14
Statistik 14
Statistik 22
Scanner 15
Wächter 14
Symbole 5
Systemanforderungen 6

V

Virendatenbanken
Aktualisierung 20
Vollständiger Scan 15

W

Wächter
Aktivierung 14
Einstellungen 14
Statistik 14
Widgets 11

© Doctor Web, 2015